Baseline Security Requirements

Santosh Chokhani

chokhani@cygnacom.com

Briefing Contents

- Motivation
- Background
- Approach
- Key Recommendations

Motivation

- **Provide Baseline Guidance to Agencies on Security Aspects of Certificate Policy and CPS**
  - Focus on Requirements to accommodate a variety of mechanisms
  - Provide examples for clarification
  - Set the baseline for basic assurance certificate policy
  - OK to exceed the baseline for the various certificate policies
- **Explain PKIX Part IV**

Background

- **Certificate Policy Framework (PKIX Part IV) Hierarchy**

Certificate Policy

Component

Subcomponent

Element

Background (concluded)

- **Components of Certificate Policy (PKIX Part IV)**
  - Introduction
  - General Provisions
  - Identification and Authentication
  - Operating Procedures
  - Physical, Procedural and Personnel Controls
  - Technical Security Controls
  - Certificate and CRL Profile
  - Specification Administration

Approach

- **Scope includes PKI Components: CA, RA, Clients**
- **For Each Element, Provide:**
  - Description
  - Security Criticality
  - Examples
  - Compliance Audit Procedure
  - Objective
  - Other Criticality
  - Baseline Recommendation
- **Above will Facilitate Agency Specific Decisions and Trade-Offs**

Key Recommendations

Applicability: e-mail, transaction < $2,500

General Provisions: Appendix, See agency General Counsel

I&A: X.500 DN, agency badging procedures, proof of private key possession, electronic rekey

Operating Procedures: archive certificate requests, certificates, revocation requests, revocations, CA key change over, archive under two person control

Key Recommendations (concluded)

- **P^3 Security Controls:** **CA in security building in access controlled computer room, separation of duties, agency secret clearance for CA, RA personnel**
- **Technical Security Controls:** **1,024 bit keys, CA private in hardware, FIPS 140-2 level 2 token, RA and client cryptographic module FIPS 140-1 level 1, 3 year certificate validity period, CA C2 equivalent and behind firewall (firewall compliant with firewall PP)**